



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,861	10/06/2003	Craig Ogg	61135/P023US/10303235	3194
29053 7590 11/02/2010 FULBRIGHT & JAWORSKI L.L.P. 2200 ROSS AVENUE SUITE 2800 DALLAS, TX 75201-2784				
EXAMINER				
ROBINSON BOYCE, AKIBA K				
ART UNIT		PAPER NUMBER		
3628				
NOTIFICATION DATE		DELIVERY MODE		
11/02/2010		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

doipdocket@fulbright.com

Office Action Summary

Application No.

10/679,861

Applicant(s)

OGG, CRAIG

Examiner

AKIBA K. ROBINSON BOYCE

Art Unit

3628

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 August 2010.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-7, 9-13, 15-22 and 29-42 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2-7, 9-13, 15-22 and 29-42 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB06)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Status of Claims

1. Due to communications filed 8/25/10, the following is a final office action. Claims 6, 7, 15, 29, 39, 41, 42 have been amended. Claims 1, 8, 14, 23-28 are cancelled. Claims 2-7, 9-13, 15-22 and 29-42 are pending in this application and have been examined on the merits. The previous rejection has been modified to reflect claim amendments.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 2-7, 9, 15-18, 34, 35, 38, 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al, (US 5,742,683).

As per claim 2, Lee et al discloses:

Wherein the user parameter comprises a maximum postage amount that the particular user is allowed to use on the meter to evidence postage (Col. 2, line 61, maximum postage amount).

As per claim 3, Lee et al discloses:

Wherein the user parameter comprises a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage, (obvious with network meter access since the user must access the meter for a certain amount of time).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention for the user parameter comprises a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage with the motivation of showing a representation of the period of access.

As per claim 4, Lee et al discloses:

wherein a first user parameter of said at least one user parameter comprises a maximum postage amount that said particular user of said plurality of users is allowed to use on the meter to evidence postage and wherein a second user parameter of said at least one user parameter comprises a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage, (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password

is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

As per claim 5, Lee et al discloses:
a user interface, (col. 4, line 26, user interface)
a printer, (col. 4, lines 34-35, non-secured digital printer); and
a security module, (col. 5, lines 14-20, encryption module).

As per claim 6, Lee et al discloses:

a removable storage device comprising an authorization database storing said at least one user parameter, (Claim 6 of Lee et al shows wherein said vault means comprises a portable vault card that is removably coupled to said PC, said PC including means for removably coupling said vault card to said PC and col. 7, line 64-col. 8, line 2, At step 120, a check is made to determine if the entered user password is authorized to perform such request. If not, the vault returns to an idle status at step 104, preferably sending a message to the user that the request is not authorized. If authorized, at steps 122-128, the requested function is performed, thereby suggesting some type of database means since in order to compare and confirm passwords the correct

passwords must be stored, where examiner interprets the entered user password as the one user parameter since user parameters are implemented with each password).

It would have been obvious to one of ordinary skill in the art to provide an authorization database with the motivation of providing means for storage of passwords.

As per claim 7, Lee et al discloses:

An authorization database storing said at least one user parameter, wherein the authorization database is coupled to the meter via a communication link to a remote postage information system (col. 3, lines 62-65, User interface module 42 also provides application programs the capability to initiate remote refills and to perform administrative functions, and col. 7, line 64-col. 8, line 2, At step 120, a check is made to determine if the entered user password is authorized to perform such request. If not, the vault returns to an idle status at step 104, preferably sending a message to the user that the request is not authorized. If authorized, at steps 122-128, the requested function is performed, thereby suggesting some type of database means since in order to compare and confirm passwords the correct passwords must be stored).

It would have been obvious to one of ordinary skill in the art to provide an authorization database with the motivation of providing means for storage of passwords.

As per claim 9, Lee et al discloses:

Wherein at least one user parameter comprises a maximum postage amount that the particular user is allowed to use on the meter to evidence postage (Col. 2, line 61, maximum postage amount).

As per claim 15, Lee et al discloses:

at least two postage evidencing meters, each meter having a processor and a communication module for providing a communication link between the at least two meters wherein each of said at least two meters store at least one postage usage meter parameter that restricts password authenticated users' usage of the respective meter storing the meter parameter, and wherein at least one postage evidencing meter of said at least two postage evidencing meters stores at least one postage usage user parameter for each user of a plurality of users, wherein each of said user parameters define meter usage limits for a particular user associated with the user parameter, (Figs 2 and 8, col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount, destination address limitations, diagnostic

and inspection report access, and departmental accounting reports via a local open metering system or a networked open metering system, col. 3, lines 5-21, shows that "Each of the modes is assigned with a user password that is required to operate the vault in the respective mode. Each user of the vault is provided with one or more passwords corresponding to the access level assigned to the user. When the vault becomes operational a normal mode password is required to place the vault in normal mode. Once operational, whenever a command is received by the vault for a function corresponding to the manufacturing mode, the service mode or the privileged mode the command must be accompanied by a respective user password. The idle time of the vault is continuously monitored so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit. The method of the present invention provides security that prevents tampering and false evidence of postage payment and provides the ability to do batch processing of digital tokens." This passage suggests restricting all password authenticated users since the vault state becomes non-operational as a result of idle time exceeding a time limit, meaning that when the time limit has not been exceeded, the vault is operable, and accessible by password authenticated users, and therefore when in a non-operational state is enforced, the password authenticated users who would normally have access, even when they try to enter in their password, are restricted to evidencing postage) ;

wherein at least one user parameter for at least one said particular user of said plurality of users is exchanged between said meters via the communication link, (col. 7,

lines 41-43, users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security, also see Fig 8); and

wherein the processor of the meter receiving said user parameter controls an ability of the particular user associated with user parameter to evidence postage using the receiving meter in accordance with the received user parameter and at least one of the meter parameters stored by the receiving meter,(col. 3, lines 5-20, Each of the modes is assigned with a user password that is required to operate the vault in the respective mode. Each user of the vault is provided with one or more passwords corresponding to the access level assigned to the user. When the vault becomes operational a normal mode password is required to place the vault in normal mode. Once operational, whenever a command is received by the vault for a function corresponding to the manufacturing mode, the service mode or the privileged mode the command must be accompanied by a respective user password. The idle time of the vault is continuously monitored so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit. The method of the present invention provides security that prevents tampering and false evidence of postage payment and provides the ability to do batch processing of digital tokens).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to disclose at least one postage usage meter parameter, wherein said meter parameter restricts all password authenticated users' of said plurality of users ability to evidence postage using the meter with the motivation of showing a state

that will restrict a user usage of the meter.

As per claim 16, Lee et al discloses:

Wherein the at least one user parameter comprises a maximum postage amount that the selected user is allowed to use on the meter to evidence postage (Col. 2, line 61, maximum postage amount).

As per claim 17, Lee et al discloses:

Wherein the at least one user parameter comprises a maximum amount of postage that can be evidenced by the selected user during a selected period of time (Col. 2, line 61, inherent with network meter access since the user must access the meter for a certain amount of time).

As per claim 18, Lee et al discloses:

wherein the a first user parameter said at least one user parameter comprises a maximum postage amount that the particular user is allowed to use on the meter to evidence postage and wherein a second user parameter of said at least one user parameter comprises a period of time during which the selected particular user is allowed to use the meter to evidence postage, (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use

associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

As per claim 34, Lee et al discloses:

wherein the at least one user parameter comprises at least one of time and amount (Col. 2, line 61, maximum postage amount).

As per claim 35, Lee et al discloses:

wherein the particular user is associated with at least two user parameters (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open

metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,).

. As per claim 38, Lee et al discloses:

wherein the at least a particular user is associated with at least two user parameters (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

As per claim 39, Lee et al discloses:

at least one postage usage meter parameter, wherein said meter parameter restricts all password authenticated users' of said plurality of users ability to evidence postage using the meter, (col. 3, lines 5-21, shows that "Each of the modes is assigned with a user password that is required to operate the vault in the respective mode. Each user of the vault is provided with one or more passwords corresponding to the access level assigned to the user. When the vault becomes operational a normal mode password is required to place the vault in normal mode. Once operational, whenever a command is received by the vault for a function corresponding to the manufacturing mode, the service mode or the privileged mode the command must be accompanied by a respective user password. The idle time of the vault is continuously monitored so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit. The method of the present invention provides security that prevents tampering and false evidence of postage payment and provides the ability to do batch processing of digital tokens." This passage suggests restricting all password authenticated users since the vault state becomes non-operational as a result of idle time exceeding a time limit, meaning that when the time limit has not been exceeded, the vault is operable, and accessible by password authenticated users, and therefore when in a non-operational state is enforced, the password authenticated users who would normally have access, even when they try to enter in their password, are restricted to evidencing postage);

at least one postage usage user parameter corresponding to a particular user of said plurality of users, wherein said user parameter limits said particular user's ability to evidence postage using the meter, and wherein each respective particular user of said plurality of users corresponds to a respective user parameter, (col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount, destination address limitations, diagnostic and inspection report access, and departmental accounting reports via a local open metering system or a networked open metering system); and

wherein said postage evidencing meter is operable to limit said particular user's ability to evidence postage using said meter in accordance with said at least one meter parameter and said at least one user parameter, (col. 7, lines 27-46, shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user of PC-based postage meter 10 to customize individual user passwords for access to the

different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to disclose at least one postage usage meter parameter, wherein said meter parameter restricts all password authenticated users' of said plurality of users ability to evidence postage using the meter with the motivation of showing a state that will restrict a user usage of the meter.

4. Claims 10, 11, 21, 29-33, 36, 37, 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al (5,742,683) and further in view of Liechti et al (US 5,715,164).

As per claim 10, Lee et al discloses:
wherein the at least one user parameter includes a period of time during which the particular user is allowed to use the meter to evidence postage (Col. 2, line 61, inherent

with network meter access since the user must access the meter for a certain amount of time).

As per claim 11, Lee et al discloses:

wherein the a first user parameter of the at least one user parameter includes a maximum postage amount that selected the particular user of said plurality of users is allowed to use on the meter to evidence postage and wherein a second user parameter of the at least one user parameter include a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage, (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

As per claim 21, Lee et al discloses:

wherein said communication link is used to transfer securely between the at least two meters using cryptographic techniques, (col. 1, line 57-col. 2, line 6, shows that typical information which may be encrypted as part of a digital token includes origination postal code, vendor identification, data identifying the PED, piece count, postage amount, date, and, for an open system, destination postal code. These items of information, collectively referred to as Postal Data, when encrypted with a secret key and printed on a mail piece provide a very high level of security which enables the detection of any attempted modification of a postal revenue block or a destination postal code. A postal revenue block is an image printed on a mail piece that includes the digital token used to provide evidence of postage payment. The Postal Data may be printed both in encrypted and unencrypted form in the postal revenue block. Postal Data serves as an input to a Digital Token Transformation which is a cryptographic transformation computation that utilizes a secret key to produce digital tokens. Results of the Digital Token Transformation, i.e., digital tokens, are available only after completion of the Accounting Process, and col. 4, lines 38-47, Electronic vault 20, which is housed in a removable card, such as PCMCIA card 30, is a secure encryption device for postage funds management, digital token generation and traditional accounting functions. PC meter system 10 may also include an optional modem 29 which is located preferably in PC 12. Modem 29 may be used for communicating with a Postal Service or a postal authenticating vendor for recharging funds (debit or credit). In an alternate embodiment the modem may be located in PCMCIA card 30.).

Lee et al does not specifically disclose wherein said at least one meter postage usage parameter is a meter balance, however, Liechti et al in col. 10, lines 18-45 shows meter balance is incorporated into the meter parameter. It would have been obvious to combine the teachings of Lee et al and Liechti et al to disclose wherein said at least one meter postage usage parameter is a meter balance with the motivation of showing that meter balance can be incorporated into evidencing of postage.

As per claim 29, Lee et al discloses:

separately storing at least one postage usage user parameter for each user of a plurality of users of a postage meter in a postage usage database, wherein said parameters establish separate postage evidencing limits for each user of said plurality of users, (col. 8, lines 41-46, users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security. PC-based postage meter 10 keeps a log, which is stored on hard drive 24, of all transactions and logins for further security, w/ lines 38-47, shows that the Electronic vault 20, is housed in a removable card, such as PCMCIA card 30, thereby making it obvious to have a database that stores a postage usage user parameter for each user of a plurality of users) ;

storing at least one postage usage meter parameter, wherein said meter parameter restricts an ability of all password authenticated users of said postage meter to evidence postage, (col. 3, lines 5-21, shows that "Each of the modes is assigned with a user

password that is required to operate the vault in the respective mode. Each user of the vault is provided with one or more passwords corresponding to the access level assigned to the user. When the vault becomes operational a normal mode password is required to place the vault in normal mode. Once operational, whenever a command is received by the vault for a function corresponding to the manufacturing mode, the service mode or the privileged mode the command must be accompanied by a respective user password. The idle time of the vault is continuously monitored so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit. The method of the present invention provides security that prevents tampering and false evidence of postage payment and provides the ability to do batch processing of digital tokens." This passage suggests restricting all password authenticated users since the vault state becomes non-operational as a result of idle time exceeding a time limit, meaning that when the time limit has not been exceeded, the vault is operable, and accessible by password authenticated users, and therefore when in a non-operational state is enforced, the password authenticated users who would normally have access, even when they try to enter in their password, are restricted to evidencing postage);

receiving a request to evidence postage from a user of said plurality of users, (col. 3, lines 29-32, performing a requested vault function when an entered user password under which the request is made has been assigned vault functional access for the

requested vault function, where col. 4, lines 19-22 shows the present invention is applicable to any-value metering system that includes a transaction evidencing.);

(a) determining, based on the requesting user's postage usage parameter, if sufficient postage is available to fulfill the request for the requesting user (col. 7, lines 27-46, shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user of PC-based postage meter 10 to customize individual user passwords for access to the different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security, where examiner interprets the password as the user parameter, where sufficient postage determination is inherent with evidencing of postage);

(b) determining based on at least one of said postage meter's meter parameters if sufficient postage is available from an available postage balance of said postage meter used for evidencing postage to fulfill the request for the requesting user (col. 7,

lines 27-46, shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user of PC-based postage meter 10 to customize individual user passwords for access to the different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security, where examiner interprets the postage limit as the meter parameter, where sufficient postage determination is inherent with evidencing of postage);

evidencing a requested postage amount if said (a) determining is affirmative and if said (b) determining is affirmative (col. 7, line 64-col. 8, line 2, At step 120, a check is made to determine if the entered user password is authorized to perform such request. If not, the vault returns to an idle status at step 104, preferably sending a message to the user that the request is not authorized. If authorized, at steps 122-128, the requested function is performed.);

It would have been obvious to provide a database that stores a postage usage user parameter for each user of a plurality of users with the motivation of showing some type of memory associated with the vault that will store user related parameters.

Lee et al does not specifically disclose the following, however, Liechti discloses:

recording postage usage for the requesting user in the postage usage database (Liechti: col. 7, lines 4-6; col. 12, lines 22-24); and

deducting an amount of postage used to fulfill the request for the requesting user from the available postage balance (Liechti: col. 7, lines 4-7).

It would have been obvious to disclose the above limitations with the motivation of showing the final steps of evidencing a postage meter.

As per claim 30, Lee et al discloses:

authenticating the requesting user (col. 8, lines 17-18, the term password is used generically and refers to present and future methods for authenticating users and col. 7, line 64-col. 8, line 2, At step 120, a check is made to determine if the entered user password is authorized to perform such request)

As per claim 31, Lee et al discloses:

receiving a request to configure parameters for the requesting user (col. 3, lines 5-20, Each of the modes is assigned with a user password that is required to operate the vault in the respective mode. Each user of the vault is provided with one or more passwords corresponding to the access level assigned to the user); and

modifying at least one of the user parameters in the postage usage database, (col. 2, lines 50-65, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password).

As per claim 32, Lee et al discloses:

the usage limit is a maximum amount of postage that can be evidenced for the requesting user (Col. 2, line 61, maximum postage amount).

As per claim 33, Lee et al discloses:

receiving a request to purchase postage for the requesting user (col. 4, lines 11-14, PC meter system 10 includes a conventional personal computer configured to operate as a host to a removable metering device or electronic vault, generally referred

to as 20, in which postage funds are stored, where the Examiner interprets storing funds on the user's account to imply receiving a request to purchase postage.); and

adding a purchased postage value to the user parameter database for the requesting user (col. 2, lines 50-65, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password).

As per claim 36, Lee et al discloses:

wherein the at least one parameter comprises at least one of time and amount (Col. 2, line 61, maximum postage amount).

As per claim 37, Lee et al discloses:

wherein the particular user is associated with at least two user parameters (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system

in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

As per claim 40, Lee et al does not specifically disclose wherein said at least one meter postage usage parameter is a meter balance, however, Liechti et al in col. 10, lines 18-45 shows meter balance is incorporated into the meter parameter. It would have been obvious to combine the teachings of Lee et al and Liechti et al to disclose wherein said at least one meter postage usage parameter is a meter balance with the motivation of showing that meter balance can be incorporated into evidencing of postage.

As per claim 41, Lee et al discloses:

a postage evidencing meter, (col. 3, line 31, shows PC-based postage meter);
a postage information system communicatively coupled to said postage evidencing meter, (col. 3, lines 41-47, PC meter system 10 may also include an optional modem 29 which is located preferably in PC 12. Modem 29 may be used for communicating with a Postal Service or a postal authenticating vendor for recharging

funds (debit or credit). In an alternate embodiment the modem may be located in PCMCIA card 30);

wherein the postage information system includes a database for separately storing at least one postage usage user parameter for a user of a plurality of users of said postage evidencing meter, wherein a particular user parameter associated with a particular user establishes usage thresholds which limit an ability of the particular user to evidence postage using the meter, and wherein each respective particular user is associated with a particular respective user parameter, ((col. 8, lines 41-46, users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security. PC-based postage meter 10 keeps a log, which is stored on hard drive 24, of all transactions and logins for further security, w/ lines 38-47, shows that the Electronic vault 20, is housed in a removable card, such as PCMCIA card 30, thereby making it obvious to have a database that stores a postage usage user parameter for each user of a plurality of users, col. 7, lines 27-46, shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user of PC-based postage meter 10 to customize individual user passwords for access to the different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are

authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security);

wherein the meter parameter establishes usage thresholds for all users of said plurality of users, (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,);

wherein said postage evidencing meter is operable to access said database through a communication module to limit the ability of said particular user of said plurality of users to evidence postage in accordance with the at least one associated particular user parameter and the at least one meter parameter, (col. 7, lines 27-46,

shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user of PC-based postage meter 10 to customize individual user passwords for access to the different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security).

It would have been obvious to provide a database that stores a postage usage user parameter for each user of a plurality of users with the motivation of showing some type of memory associated with the vault that will store user related parameters.

Lee et al does not specifically disclose wherein the database also includes at least one postage usage meter parameter, however, Liechti et al in col. 10, lines 18-45 shows meter balance is incorporated into the meter parameter. It would have been obvious to combine the teachings of Lee et al and Liechti et al to disclose wherein said

at least one meter postage usage parameter is a meter balance with the motivation of showing that meter balance can be incorporated into evidencing of postage.

As per claim 42, Lee et al does not specifically disclose wherein said at least one meter postage usage parameter is a meter balance, however, Liechti et al in col. 10, lines 18-45 shows meter balance is incorporated into the meter parameter. It would have been obvious to combine the teachings of Lee et al and Liechti et al to disclose wherein said at least one meter postage usage parameter is a meter balance with the motivation of showing that meter balance can be incorporated into evidencing of postage.

5. Claims 12, 13, 19, 20, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al and further in view of Manduley, U.S. Publication No. (US

Art Unit: 3628

2004/0098354).

As per claim 12, Lee et al does not teach the communication link is a wireless link,

Manduley teaches the communication link is a wireless link (Manduley: paragraph 0039). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al to have included the communication link is a wireless link as taught by Manduley for the advantage of providing a convenient way for postage meters to communicate with one another.

As per claim 13, Lee et al fails to disclose wherein the communications link is a wireline link, however, Manduley teaches in [0039] that the connection between two postal meters 100.sub.a and 100.sub.b, as shown in FIGS. 3a and 3b, can be wired or wireless.

It would have been prima facie obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al and further in view of Manduley to have included as taught by Manduley for the advantage of providing a convenient way for postage meters to communicate with one another.

As per claim 19, Lee et al does not teach the communication link is a wireless link.

Manduley further teaches the communication link is a wireless link (Manduley: paragraph 0039).

It would have been prima facie obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al and further in view of Manduley to have included the communication link is a wireless link as taught by Manduley for the advantage of providing a convenient way for postage meters to communicate with one another.

As per claim 20, Lee et al fails to disclose wherein the communications link is a wireline link, however, Manduley teaches in [0039] that the connection between two postal meters 100.sub.a and 100.sub.b, as shown in FIGS. 3a and 3b, can be wired or wireless.

It would have been prima facie obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al and further in view of Manduley to have included as taught by Manduley for the advantage of providing a convenient way for postage meters to communicate with one another.

As per claim 22, Lee et al does not teach an exchange between two meters is bi-directional.

Manduley further teaches an exchange between two meters is bi-directional (Manduley: paragraphs 0034-0037 - The Examiner notes, one meter can send funds to another meter and vice versa.). It would have been prima facie obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al

and further in view of Manduley to have included an exchange between two meters is bi-directional as taught by Manduley for the advantage of effectively transmitting and updating data between meters without the need for connecting to a remote data center.

Response to Arguments

6. Applicant's arguments, see Arguments/Remarks, filed 8/25/10, with respect to claims 2-7, 9-13, 15-22 and 29-42 have been fully considered and are persuasive. The 35 U.S.C. § 112 Rejection of claims 6 and 7 has been withdrawn.

7. Examiner notes that as a result of the amendment filed 4/12/10, claims 10 and 11 should have been rejected as dependents of claim 41, however, have been inadvertently placed under section 3 of this office action as being rejected as a dependent of claim 8 (as they originally were). Examiner notes that the scope of the rejection has not changed, However, for clarity purposes, examiner has now placed claims 10 and 11 under the section 6 as being rejected as dependents of claim 41.

8. Applicant's arguments filed 8/25/10 have been fully considered but they are not persuasive.

As per claim 10, applicant specifically argues that "Claim 10 recites "the at least one user parameter comprises: a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage." The *Office Action* cites to column 2, line 61 of *Lee* and states that the claim is inherently taught by *Lee*

since the user must access the meter for a certain amount of time. However, the *Office Action's* analysis is flawed. Column 2, line 61 of *Lee* does not teach a time limitation. Instead, *Lee* discloses that customized features can be "vault refill, network meter access, maximum postage amount, destination address limitations, diagnostic and inspection repost access, and departmental accounting records." No time limitation is taught. However, examiner disagrees. It is only once a password is entered in by a user before the vault can be accessed, and these customized features be available, and since *Lee* discloses that "each of the users have different access privileges, includes programming a vault with a plurality of operational modes...Each of the modes is assigned with a user password that is required to operate the vault in the respective mode... The idle time of the vault is continuously monitored so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit" as shown in col. 2, line 66-col. 3, line 16, this shows that when a user inputs a password for network meter access, idle time is being monitored. Therefore, for the network meter access feature, when enforced, this idle time represents "a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage" since "if the continuous idle time exceeds an idle time limit, the vault is placed in an non-operational state" as shown in col. 3, lines 14-16, and the user therefore would not be able to use the meter at this time.

Applicant further argues that claim 11 requires "a second user parameter of the at least one user parameter include a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage." However,

examiner maintains her argument for at least the same reasons as disclosed above with respect to claim 10.

As per claim 39, applicant argues that "Amended claim 39 requires "at least one postage usage meter parameter, wherein said meter parameter restricts all password authenticated users' of said plurality of users ability to evidence postage using the meter..." and that "the password of *Lee* does not prevent a valid user from evidencing postage. The password merely delays users by adding an extra step. Thus, *Lee*'s password is distinct from the claimed meter parameter, which because, in *Lee*, the user has the ability to move forward by inputting the password. In contrast, the claimed meter parameter restricts a user's ability to move forward. As such, *Lee* fails to teach "at least one postage usage meter parameter, wherein said meter parameter restricts all password authenticated users' of said plurality of users ability to evidence postage using the meter" (emphasis added)." However, examiner disagrees. Although true that the user has ability to move forward by inputting a password, the users ability is still restricted to move forward if the user does not present this password. As disclosed above in the rejection, col. 3, lines 5-21, shows that "Each of the modes is assigned with a user password that is required to operate the vault in the respective mode. Each user of the vault is provided with one or more passwords corresponding to the access level assigned to the user. When the vault becomes operational a normal mode password is required to place the vault in normal mode. Once operational, whenever a command is received by the vault for a function corresponding to the manufacturing mode, the service mode or the privileged mode the command must be

accompanied by a respective user password. The idle time of the vault is continuously monitored so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit. The method of the present invention provides security that prevents tampering and false evidence of postage payment and provides the ability to do batch processing of digital tokens." This passage suggests restricting all password authenticated users since the vault state becomes non-operational as a result of idle time exceeding a time limit, meaning that when the time limit has not been exceeded, the vault is operable, and accessible by password authenticated users, and therefore when in a non-operational state is enforced, the password authenticated users who would normally have access, even when they try to enter in their password, are restricted to evidencing postage.

Dependent claims 2-5 and 34-35 depend from independent claim 39 thereby inheriting the limitations therein, and are therefore still rejected for the same reasons as discussed above with respect to claim 39.

Applicant further argues that claim 15 recites "at least one postage usage meter parameter that restricts password authenticated users' usage of the respective meter storing the meter parameter" The Office Action cites to column 2, lines 50-65 as teaching a user parameter and likens the parameter to Lee's requirement of a user password. Office Action at 7-9. As explained above, regarding claim 39, Lee's password does not restrict a user's usage of a meter. Rather, the password requirement merely delays the user's access due to the required extra step. However, examiner still

maintains her rejection for the same reasons as discussed above with respect to claim 39.

With regard to claim 15, applicant further argues that "Claim 15 also requires "wherein the processor of the meter receiving said user parameter controls an ability of the particular user associated with the user parameter to evidence postage using the receiving meter in accordance with the received user parameter and at least one of the meter parameters stored by the receiving meter." The *Office Action* relies on column 2, lines 50-65 as teaching the user parameter and figure 8 as teaching the receiving meter controlling an ability of the particular user to evidence postage. *Office Action* at 7-9. However, the line of figure 8, does not teach the limitation. As explained above, figure 8, and the description thereof(col. 8, lines. 6-16), simply does not provide any description of what this line is or what this line does. Thus, this line does not provide adequate detail to anticipate wherein the processor of the meter receiving said user parameter controls an ability of the particular user associated with the user parameter to evidence postage using the receiving meter in accordance with the received user parameter and at least one of the meter parameters stored by the receiving meter." However, examiner does not rely on col. 2, lines 50-65 or Fig. 8 to teach this limitation. Examiner relied on col. 3, lines 5-20, to teach "wherein the processor of the meter receiving said user parameter controls an ability of the particular user associated with the user parameter to evidence postage using the receiving meter in accordance with the received user parameter and at least one of the meter parameters stored by the receiving meter." It is here that Lee et al teaches "Each of the modes is assigned with

a user password that is required to operate the vault in the respective mode. Each user of the vault is provided with one or more passwords corresponding to the access level assigned to the user. When the vault becomes operational a normal mode password is required to place the vault in normal mode. Once operational, whenever a command is received by the vault for a function corresponding to the manufacturing mode, the service mode or the privileged mode the command must be accompanied by a respective user password. The idle time of the vault is continuously monitored so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit. The method of the present invention provides security that prevents tampering and false evidence of postage payment and provides the ability to do batch processing of digital tokens". In this case, the user parameters of the present invention is represented by the users password ability, and the meter parameters are represented by idle time limit of the meter.

Dependent claims 16-18 and 3 8 depend from independent claim 15 thereby inheriting the limitations therein, and are therefore still rejected for the same reasons as disclosed above with respect to claim 15.

As per claim 29, examiner maintains her rejection for the same reasons as disclosed above with respect to claims 39 and 15.

Further, applicant argues that claim 29 requires "evidencing a requested postage amount if said (a) determining is affirmative and if said (b) determining is affirmative [determining, based on at least one of said postage meter's meter parameters, if

sufficient postage is available]" (emphasis added), and argues that *Lee* does not teach evidencing a requested postage amount if said (b) determining is affirmative, rather, only checks if the user has permission for the transaction. However, because the operability of the meter depends on determining if an Idle state is over a limit, as already disclosed above in the rejection and arguments, evidencing...if said determining is affirmative...based on at least one of said postage meter's meter parameters is suggested since postage would not be able to be evidenced if the Idle state goes over a limit and the operation of the vault, and therefore, the ability to determine if sufficient postage is available would not be affirmative.

Further, applicant argues that claim 41 requires "at least one postage usage meter parameter, wherein the meter parameter establishes usage thresholds for all users of said plurality of users" (emphasis added), and that *Lee* does not teach a postage usage meter parameter that establishes usage thresholds. Applicant argues that the password merely delays users by adding an extra step and does not establish a usage threshold for all users. However, examiner disagrees. Since *Lee et al* discloses that users have different access privileges that depend on the user's password, as disclosed in col. 3, lines 1-20, this represents a usage threshold since these privileges correspond to operational modes of the vault, which are assigned a hierarchy. In addition, since *Lee et al* discloses the idle time exceeds an idle time limit, this meter parameter defines a usage threshold since *Lee et al* suggest that during idle time, while the vault is operational, users have the ability to enter in their passwords and to the system.

Furthermore, claim 41 is still rejected for the same reasons as disclosed above with respect to claims 39 and 15.

Dependent claims 21 and 40 depend from independent claims 15 and 39, respectively, and are therefore still rejected for the same reasons as disclosed with respect to claims 15 and 39..

Dependent claims 3, 6, and 7 depend from independent claim 39 thereby inheriting the limitations therein, and are therefore still rejected for the same reasons as claim 39.

Dependent claims 12, 13, 19, 20, and 22 depend from independent claims 41 and 15, respectively, thereby inheriting the limitations therein, and are therefore still rejected for the same reasons as claims 41 and 15.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Akiba K Robinson-Boyce whose telephone number is 571-272-6734. The examiner can normally be reached on Monday-Friday 9am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Hayes can be reached on 571-272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the •Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business

Art Unit: 3628

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

A. R. B.
October 28, 2010

/Akiba K Robinson-Boyce/
Primary Examiner, Art Unit 3628